PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345798
(43)Date of publication of application : 14.12.2001

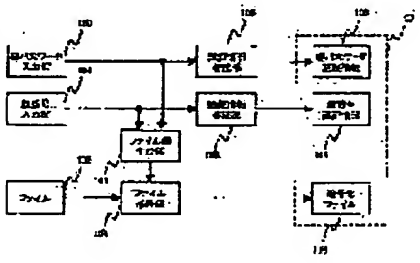
(51)Int.Cl. H04L 9/08
G06F 1/00
G06F 12/00
G06F 12/14
G09C 1/00

(21)Application number : 2000-162036
(22)Date of filing : 31.05.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : INAGAKI SATORU
KOYAMA KAZUHIRO
EMURA SATOSHI
HIDAKA NORIYUKI
MATSUZAKI NATSUME

(54) APPARATUS FOR ENCRYPTING/DECRYPTING FILE

(57)Abstract:
PROBLEM TO BE SOLVED: To overcome the problem of a conventional apparatus for encrypting/ decrypting a file using a password such that a password must be inputted every time when a file is encrypted or decrypted, and the problem of an conventional apparatus for encrypting/decrypting a file using a memory card that it is difficult to decrypt the file when the memory card is missed.
SOLUTION: A key password and a key number stored on a memory card are read in from a key password input section 100 and a key number input section 101. An encryption key is generated, based on them and a file is encrypted. An encrypted file can be decrypted by inserting the memory card storing the key password or the key number, or by inputting the key password and the key number.



LEGAL STATUS

[Date of request for examination]	08.01.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	withdrawal
[Date of final disposal for application]	11.05.2005
[Patent number]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－345796
（P2001－345796A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04L	9/08		G06F	1/00	370E	5B017
G06F	1/00	370		12/00	537H	5B082
	12/00	537		12/14	320B	5J104
	12/14	320			320C	
			G09C	1/00	630Z	

審査請求　未請求　請求項の数24　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2000－162036(P2000－162036)

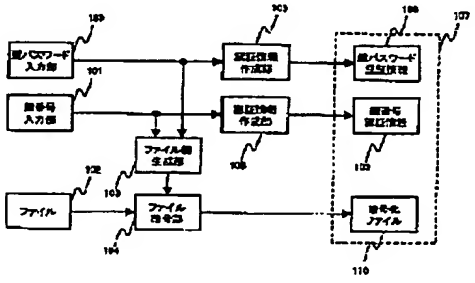
(22)出願日　平成12年５月31日(2000.5.31)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　稲垣　悟
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　小山　和弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　ファイル暗号復号装置

(57)【要約】
【課題】　従来、パスワードによる暗号復号装置においては、ファイルの暗号や復号処理を行うたびにパスワードを入力する必要があった。またメモリカード等を利用した暗号復号装置においては、メモリカードの紛失により、ファイルの復号が困難になるといった課題があった。
【解決手段】　鍵パスワード入力部１００と鍵番号入力部１０１とから、メモリカード上に格納された鍵パスワードと鍵番号とが読み込まれる。これらに基づき暗号鍵が生成され、ファイルが暗号化される。復号時には、鍵パスワードもしくは暗号鍵が格納されたメモリカードを挿入するか、鍵パスワードと鍵番号とを入力することにより暗号ファイルを復号化することができる。



1

【特許請求の範囲】

【請求項１】 ファイルを入力するファイル入力手段と、

鍵パスワードを入力する鍵パスワード入力手段と、

鍵生成情報を入力する鍵生成情報入力手段と、

前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、

前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたことを特徴とするファイル暗号装置。

【請求項２】 暗号化ファイルを入力とし、

鍵パスワードを入力する鍵パスワード入力手段と、

鍵生成情報を入力する鍵生成情報入力手段と、

前記鍵パスワードと前記鍵生成情報とに基づき、ファイル鍵を生成するファイル鍵生成手段と、

前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたことを特徴とするファイル復号装置。

【請求項３】 前記ファイル暗号手段は、前記鍵パスワードの認証情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置において、前記認証情報を用いて前記鍵パスワード入力手段から入力された鍵パスワードの認証を行う認証手段を備えたことを特徴とする請求項１または請求項２記載のファイル暗号復号装置。

【請求項４】 前記ファイル暗号手段は、前記鍵生成情報の認証情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置において、前記認証情報を用いて前記鍵生成情報入力手段から入力された鍵生成情報の認証を行う認証手段を備えたことを特徴とする請求項１または請求項２記載のファイル暗号復号装置。

【請求項５】 前記ファイル暗号手段は、前記鍵生成情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置における鍵生成情報入力手段は、前記暗号化ファイルのヘッダから鍵生成情報を抽出することを特徴とする請求項１または請求項２記載のファイル暗号復号装置。

【請求項６】 前記ファイル鍵生成情報は、所定の暗号鍵で暗号化されてヘッダに添付されることを特徴とする請求項５記載のファイル暗号復号装置。

【請求項７】 前記鍵パスワードを可搬媒体に格納し、

前記鍵パスワード入力手段は、前記可搬媒体に格納された鍵パスワードを読み込むことを特徴とする請求項１または請求項２記載のファイル暗号復号装置。

【請求項８】 ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、

ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、

ファイルを入力するファイル入力手段と、

鍵生成情報を入力する鍵生成情報入力手段と、

2

前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、

前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、

前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたことを特徴とするファイル暗号装置。

【請求項９】 暗号化ファイルを入力とし、

ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、

ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、

鍵生成情報を入力する鍵生成情報入力手段と、

前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、

前記鍵パスワードと前記鍵番号とに基づき、ファイル鍵を生成するファイル鍵生成手段と、

前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたことを特徴とするファイル復号装置。

【請求項１０】 前記ファイル暗号手段は、前記鍵生成情報の認証情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置において、前記認証情報を用いて前記鍵生成情報入力手段から入力された鍵生成情報の認証を行う認証手段を備えたことを特徴とする請求項８または請求項９記載のファイル暗号復号装置。

【請求項１１】 前記ファイル暗号手段は、前記鍵生成情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置における鍵生成情報入力手段は、前記暗号化ファイルのヘッダから鍵生成情報を抽出することを特徴とする請求項８または請求項９記載のファイル暗号復号装置。

【請求項１２】 前記ファイル鍵生成情報は、所定の暗号鍵で暗号化されてヘッダに添付されることを特徴とする請求項１１記載のファイル暗号復号装置。

【請求項１３】 前記ユーザ情報または鍵生成情報とを可搬媒体に格納し、前記ユーザ情報入力手段または鍵生成情報入力手段は、前記可搬媒体に格納されたユーザ情報または鍵生成情報を読み込むことを特徴とする請求項８または請求項９記載のファイル暗号復号装置。

【請求項１４】 前記鍵パスワードを可搬媒体に格納し、前記ファイル鍵生成手段において、前記可搬媒体から鍵パスワードが入力されることを特徴とする請求項９記載のファイル復号装置。

【請求項１５】 前記鍵生成情報は、鍵の種類を表す鍵番号であることを特徴とする請求項１または請求項２または請求項９または請求項１０記載のファイル暗号復号装置。

【請求項１６】 前記ファイル鍵生成手段は、前記鍵パ

スワードを第１の暗号化鍵に変換する鍵パスワード変換手段を備え、前記鍵番号をＮとしたときに、前記第１の暗号化鍵に対して、所定の関数でＮ回変換を行い、ファイル鍵として出力することを特徴とする請求項１５記載のファイル暗号復号装置。

【請求項１７】　前記鍵生成情報は、暗号化ファイルの格納場所情報であることを特徴とする請求項１または請求項２または請求項８または請求項９記載のファイル暗号復号装置。

【請求項１８】　前記ファイル暗号装置において、暗号化ファイルの格納場所を指定する格納場所指定手段を備え、前記格納場所指定手段で指定された格納場所情報が前記鍵生成情報入力手段から入力されることを特徴とする請求項１７記載のファイル暗号復号装置。

【請求項１９】　前記ファイル復号装置において、暗号化ファイルの格納場所を検出する格納場所検出手段を備え、前期格納場所検出手段で検出された格納場所情報が、前記鍵生成情報入力手段から入力されることを特徴とする請求項１７記載のファイル暗号復号装置。

【請求項２０】　前記ファイル鍵生成手段は、前記鍵パスワードを第１の暗号化鍵に変換する鍵パスワード変換手段と、

前記格納場所情報を第２の暗号化鍵に変換する格納場所情報変換手段とを備え、

前記第１の暗号化鍵と前記第２の暗号化鍵とを所定の関数で変換し、ファイル鍵として出力することを特徴とする請求項１７記載のファイル暗号復号装置。

【請求項２１】　前記鍵生成情報は、装置のシリアル番号であることを特徴とする請求項１または請求項２または請求項８または請求項９記載のファイル暗号復号装置。

【請求項２２】　装置のシリアル番号を抽出し、前記鍵生成情報入力手段に対してシリアル番号を送出するシリアル番号抽出手段を備えたことを特徴とする請求項２１記載のファイル暗号復号装置。

【請求項２３】　前記ファイル鍵生成手段は、前記鍵パスワードを第１の暗号化鍵に変換する鍵パスワード変換手段と、

前記シリアル番号を第２の暗号化鍵に変換するシリアル番号変換手段とを備え、

前記第１の暗号化鍵と前記第２の暗号化鍵とを所定の関数で変換し、ファイル鍵として出力することを特徴とする請求項２１記載のファイル暗号復号装置。

【請求項２４】　複数ユーザが使用する場合において、

マスタユーザと一般ユーザとを規定し、

マスタユーザがマスタユーザの鍵パスワードに基づきマスタユーザ用の前記第１の暗号化鍵を生成し、

一般ユーザは一般ユーザの鍵パスワードと前記マスタユーザの鍵パスワードとに基づき一般ユーザ用の前記第１の暗号鍵を生成することを特徴とする請求項１６または請求項２０または請求項２３記載のファイル暗号復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、計算機に付随した鍵情報を用いたファイルの暗号復号装置に関する。

【０００２】

【従来の技術】従来のファイル暗号復号装置では、パスワードの入力もしくはＩＣカードなどにより、ファイルの暗号および復号が行われていた。しかしながらパスワードによる方法では、ファイルの暗号・復号を行うたびにパスワードを要求されるためユーザに負担がかかるといった問題点があった。またパスワードもしくはＩＣカードによる方法でも、複数の暗号鍵を用いる場合に暗号鍵の管理が煩雑になるといった問題点があった。

【０００３】この問題を解決するための従来のファイル暗号復号装置としては、例えば特開平９－２０４３３０号公報に記載されたものが知られている。このファイル暗号復号装置においては、ある暗号鍵を用いて暗号化されたファイルが、ディスク上の特定のフォルダ（先行文献では暗号フォルダと定義されているので、以下暗号フォルダという）に格納される。

【０００４】暗号フォルダはあらかじめユーザにより作成され、認証用パスワードが設定される。これにより、暗号フォルダへのアクセス制御が行われる。また、暗号フォルダごとに暗号鍵生成用の任意数値が設定され、この数値と前記認証用パスワードとからファイル暗号用鍵が自動生成される。このファイル暗号用鍵によりファイルが暗号化され、暗号フォルダに格納される。

【０００５】これにより、パスワードの入力なしに、ファイルの暗号化や復号化を行うことができる。

【０００６】

【発明が解決しようとする課題】しかしながら従来の方法では、暗号フォルダに保存されている認証用パスワードファイルまたは暗号鍵生成用の任意数値を格納したファイルが、何らかの要因で破損した場合、暗号化されたファイルを復旧することは困難であるという課題がある。

【０００７】本発明は、簡易な操作でファイルの暗号復号処理を行うことができ、かつ緊急時にはパスワードによるファイルの復号が可能であるファイル暗号復号装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】この課題を解決するために、請求項１記載の発明は、ファイルを入力するファイル入力手段と、鍵パスワードを入力する鍵パスワード入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出

力するファイル暗号手段とを備えたものである。

【０００９】また請求項２記載の発明は、暗号化ファイルを入力とし、鍵パスワードを入力する鍵パスワード入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記鍵パスワードと前記鍵生成情報とに基づき、ファイル鍵を生成するファイル鍵生成手段と、前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたものである。

【００１０】また請求項８記載の発明は、ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、ファイルを入力するファイル入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたものである。

【００１１】また請求項９記載の発明は、暗号化ファイルを入力とし、ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、前記鍵パスワードと前記鍵番号とに基づき、ファイル鍵を生成するファイル鍵生成手段と、前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたものである。

【００１２】また請求項１４記載の発明は、前記鍵パスワードを可搬媒体に格納し、前記ファイル鍵生成手段において、前記可搬媒体から鍵パスワードが入力されることを特徴とするものである。

【００１３】また請求項１５記載の発明は、前記鍵生成情報が、鍵の種類を表す鍵番号であることを特徴とするものである。

【００１４】また請求項１６記載の発明は、前記ファイル鍵生成手段が、前記鍵パスワードを第１の暗号化鍵に変換する鍵パスワード変換手段を備え、前記鍵番号をNとしたときに、前記第１の暗号化鍵に対して、所定の関数でN回変換を行い、ファイル鍵として出力することを特徴とするものである。

【００１５】また請求項１７記載の発明は、前記鍵生成情報が、暗号化ファイルの格納場所情報であることを特徴とするものである。

【００１６】また請求項２１記載の発明は、前記鍵生成情報が、装置のシリアル番号であることを特徴とするものである。

【００１７】また請求項２４記載の発明は、複数ユーザ

が使用する場合において、マスタユーザと一般ユーザとを規定し、マスタユーザがマスタユーザの鍵パスワードに基づきマスタユーザ用の前記第１の暗号化鍵を生成し、一般ユーザは一般ユーザの鍵パスワードと前記マスタユーザの鍵パスワードとに基づき一般ユーザ用の前記第１の暗号鍵を生成することを特徴とするものである。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。

【００１９】（実施の形態１）図１は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、１００は鍵パスワードを入力する鍵パスワード入力部、１０１は鍵番号を入力する鍵番号入力部、１０２は暗号化したいファイル、１０３は前記鍵パスワードと前記鍵番号とからファイルを暗号化するためのファイル鍵を生成するファイル鍵生成部、１０４は前記ファイル鍵により前記ファイルを暗号化するファイル暗号部、１０５および１０６は前記鍵パスワードと前記鍵番号の認証情報を作成する認証情報作成部、１０７はヘッダも含めた暗号ファイル、１０８および１０９は鍵パスワードおよび鍵番号の認証情報、１１０は暗号化ファイルである。

【００２０】図２は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図１と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図２において、２００は鍵パスワードを入力する鍵パスワード入力部、２０１は鍵番号を入力する鍵番号入力部、２０２は入力された鍵パスワードと鍵番号とを認証する認証部、２０３は鍵パスワードと鍵番号とからファイル鍵を生成するファイル鍵生成部、２０４はファイルを復号するファイル復号部、２０５は復号されたファイルである。

【００２１】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【００２２】まずユーザが暗号化したいファイルの選択を行い、鍵パスワードの入力を行う。鍵パスワードはユーザが任意に設定することができる。単純な数文字程度のパスワードでもよいし、数十文字の長いパスワードでもよい。パスワードの入力は、通常あらかじめパスワードを格納しておいた記憶媒体から行われるものとする。本発明のファイル暗号復号装置にメモリカード等を挿入するスロットを備え、スロットに挿入されたメモリカードから鍵パスワードを読み込む仕組みを備えることで実現できる。もちろん、キーボード等の入力装置から鍵パスワードを入力してもよい。

【００２３】鍵パスワードの入力が行われると、次に鍵番号が入力される。鍵番号は、例えば図３のようにファイルの使用目的毎に鍵を変えて暗号化するために用いられる。例えば鍵パスワードを、ある文字列もしくは数値列「Ａ」は会社で使用するファイルと規定し、鍵番号

「１」は自分専用、鍵番号「２」はプロジェクト用、鍵番号「Ｎ」は連絡事項用のファイルを暗号化する際に用いる。これにより暗号化されたファイルを鍵番号で管理することができる。

【００２４】鍵パスワードと鍵番号とが入力されるとファイル鍵生成部１０３でファイル暗号用の鍵であるファイル鍵が生成される。ファイル鍵は、例えばｎ文字以上の文字列をｍビットの数値列に変換する関数と、ｍビット数値列の並びを変えたｍビット数値列に変換する関数とを組み合わせることで生成される。鍵生成の流れを図４に示す。図４においてＳ４００はｎ文字以上の文字列をｍビットの数値列に変換するステップであり、Ｓ４０１はｍビット数値列の並びを変える変換を行うステップである。鍵パスワードがｎ文字以上であればＳ４００のステップへ入り、鍵パスワードがｎ文字以下の場合は所定のビットを追加してからＳ４００のステップへ入る。次に鍵番号に応じてＳ４０１のステップが繰り返される。鍵番号が１であればＳ４０１の処理が一度だけ行われるが、鍵番号がＮであれば、Ｓ４０１の処理がＮ回繰り返される。この結果ファイル鍵がｍビットの数値列として出力される。

【００２５】ファイル鍵生成部１０３でファイル鍵が生成されると、ファイル暗号部１０４でファイルが暗号化される。暗号化の方法はいかなるものでもよく、暗号アルゴリズムが必要とするファイル鍵のビット数に応じて、ファイル鍵生成部１０３で生成されるファイル鍵のビット数が決定される。

【００２６】認証情報作成部１０５および１０６では、鍵パスワードおよび鍵番号のハッシュ値が鍵パスワード認証情報および鍵番号認証情報として出力される。暗号ファイル１０７には、ファイル暗号部１０４の出力である暗号化ファイルに、前記鍵パスワード認証情報１０８および鍵番号認証情報１０９がヘッダとして添付される。

【００２７】次に復号処理について説明する。図２において、暗号ファイル１０７を入力とし、認証部２０２において鍵パスワード認証情報１０８および鍵番号認証情報１０９が抽出される。次にこのファイルを復号化するための鍵パスワードと鍵番号とを鍵パスワード入力部２００および鍵番号入力部２０１から入力する。鍵パスワードは通常メモリカード等を挿入することで入力されるが、キーボード等の入力手段から入力される場合のみ暗号処理、復号処理を可能とすることにより、登録されたメモリカードの悪用を防ぐことができる。この場合、メモリカード上には、所定の変換関数により変換した鍵パスワードを格納することにより、安全性を増すことができる。

ドまたは鍵番号が正しくないと判断されれば、ファイル復号部２０４における復号処理は行われない。

【００２８】なお、鍵パスワード入力部１００および２００において、メモリカードによる手段とキーボード等の入力手段のいずれでもよいとしたが、どちらか片方に制限してもよい。例えば鍵パスワードが意に反して漏洩した場合には、メモリカードが挿入されている場合のみ暗号処理、復号処理を可能とすることにより、キーボードからパスワードを入力されることを防止できる。また、メモリカードを紛失した場合には、キーボード等の入力手段から入力される場合のみ暗号処理、復号処理を可能とすることにより、登録されたメモリカードの悪用を防ぐことができる。この場合、メモリカード上には、所定の変換関数により変換した鍵パスワードを格納することにより、安全性を増すことができる。

【００２９】また、鍵番号入力部１０１からは鍵の番号を入力するとして説明したが、任意の文字列を用いてもよい。この場合、任意の文字列を固定ビットの数値に変換する関数を設けて、図４におけるＫの値を設定すればよい。例えば任意の文字列を８ビットの数値に変換した場合、Ｋの値は１から２５６のいずれかの値をとることになる。

【００３０】（実施の形態２）図５は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図１と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図５において、５００は鍵番号を暗号化する暗号処理部、５０１は鍵番号が暗号化された鍵番号情報である。

【００３１】図６は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図１、図２、図５と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図６において、６００は暗号ファイル１０７のヘッダ部にある鍵パスワード認証情報を抽出し、鍵パスワード入力部２００で入力された鍵パスワードの認証を行う認証部、６０１は鍵番号情報５０１の復号処理を行い、鍵番号を出力する復号処理部、６０２は鍵パスワードと鍵番号とからファイル鍵を生成するファイル鍵生成部である。

【００３２】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【００３３】鍵パスワードが格納されたメモリカードを

ァイル１０７のヘッダ部に添付される。実施の形態１では、暗号ファイル１０７の中に鍵番号の認証情報をヘッダとして添付したのに対して、実施の形態２では、鍵番号そのものを暗号化してヘッダに添付する点で異なっている。

【００３４】次に復号処理について説明する。ユーザがメモリカードを挿入すると、鍵パスワード入力部２００においてメモリカード上の鍵パスワードが読み込まれる。認証部６００では、入力された鍵パスワードと暗号ファイル１０７のヘッダに添付された鍵パスワード認証情報１０８とが比較される。復号処理部６０１では暗号ファイル１０７のヘッダに添付された鍵番号情報５０１（暗号化された鍵番号）から、所定の鍵で復号化して鍵番号を取り出す。認証部６００において、入力された鍵パスワードが正しいと判断されれば、ファイル鍵生成部６０２においてファイル鍵が生成され、ファイル復号部２０４で復号処理が行われる。認証部６００において入力された鍵パスワードが正しくないと判断された場合には、ファイル鍵生成部６０２で鍵が生成されず、ファイルの復号は行われない。この場合、正しいパスワードの入力を促すメッセージを表示しながら、鍵パスワード入力待ち状態を保ってもよい。

【００３５】実施の形態１では、ファイルの復号時に、暗号ファイルに対してどの鍵を使用したのかを指定する必要があったが、実施の形態２ではファイル復号時に鍵番号の指定が不要である。

【００３６】（実施の形態３）図７は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図１と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図７において、７００は暗号ファイルの格納場所を指定する格納場所指定部、７０１は鍵パスワードと格納場所情報とからファイル鍵を生成するファイル鍵生成部、７０２は格納場所の認証情報を作成する認証情報作成部、７０３は格納場所の認証情報である。

【００３７】図８は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図２および図６と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図８において、８００は暗号ファイルの格納場所を抽出する格納場所抽出部、８０１は格納場所抽出部で抽出された格納場所情報と、暗号ファイル内の格納場所認証情報７０３とを比較する認証部、８０２は鍵パスワードと格納場所情報とからファイル鍵を生成するファイル鍵生成部である。

【００３８】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【００３９】まず暗号処理について述べる。図７において、格納場所指定部７００では暗号化されたファイルの保存場所の指定を行う。指定方法は、直接フォルダ名を入力してもよいし、ＧＵＩなどによるマウスを用いた方法でもよい。ここで格納場所指定部７００の出力は、例えば暗号ファイルを格納するディレクトリの絶対パスの情報などである。暗号ファイルの格納場所が指定されると、ファイル鍵生成部７０１において、鍵パスワードと格納場所情報とに基づきファイル鍵が生成される。ファイル鍵は、例えば図９のような流れで生成される。鍵パスワードをｎ文字以上に変換した後、ｍビットの数値列に変換し、これをＣ１とする。（Ｓ９００）次に格納場所情報をｎ文字以上に変換した後、ｍビットの数値列に変換し、これをＣ２とする。（Ｓ９０１）次にＣ１とＣ２との間で所定の演算を行い（Ｓ９０２）、ファイル鍵を生成する。

【００４０】ファイル鍵が生成されると、ファイル暗号部１０４にてファイルが暗号化される。認証情報作成部１０５では鍵パスワードの認証情報が作成される。認証情報作成部７０２では、格納場所情報の認証情報が作成される。

【００４１】実施の形態１および２では、鍵番号により使用する鍵を管理していたが、実施の形態３では、鍵の種類を変化させるために、暗号ファイルの格納場所の情報を用いている。この様子を図１０に示す。鍵番号で管理する場合は図３に示したように、鍵パスワードと鍵番号のテーブルにより管理が行われる。本実施の形態では、図１０に示すように、ファイルの使用目的と格納フォルダ名とを関連付けることにより、ファイルの保存フォルダに基づき鍵管理を行うことができる。

【００４２】次に復号処理について述べる。図８において、鍵パスワード入力部２００から鍵パスワードが入力されると、認証部６００において入力された鍵パスワードの認証が行われる。次に格納場所抽出部８００において、暗号ファイル１０７の格納場所が抽出される。たとえば暗号ファイル１０７が保存されている絶対パスの情報などである。次に認証部８０１において、格納場所抽出部８００で得られた格納場所情報の認証が行われる。

【００４３】認証の結果、格納場所抽出部８００で得られた格納場所と格納場所認証情報７０３とが一致した場合、すなわち復号時の格納場所が、暗号時の格納場所と同じ場合、格納場所情報がファイル鍵生成部８０２に入力される。認証部８０１での認証の結果、暗号時の格納場所と異なっている場合は、ファイル鍵生成部８０２には、認証に失敗したという情報が入力され、ファイル鍵は生成されない。

【００４４】ここで、格納場所情報の認証に失敗した場合、ユーザがキーボード等の手段により格納場所情報を入力できるように設定してもよいし、認証に失敗した場合は復号不能という設定にしてもよい。認証に失敗した場合に復号不能とすれば、例えば他のディレクトリへ暗号ファイルをコピーすれば、復号不能となるので、ファイルコピーに対するセキュリティレベルを向上できるというメリットも生じる。

【００４５】（実施の形態４）図１１は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図７と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図１１において、１１００は格納場所指定部７００で指定された格納場所情報を所定の暗号鍵で暗号化する暗号処理部、１１０１は暗号化された格納場所情報である。

【００４６】図１２は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図８と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図１２において、１２００は暗号ファイル１０７のヘッダ部に添付された格納場所情報１１０１を所定の暗号鍵で復号化する復号処理部である。

【００４７】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【００４８】まず、暗号処理について述べる。鍵パスワード入力部１００において、例えばメモリカードから鍵パスワードが読み込まれる。次に格納場所指定部７００から、暗号ファイルの格納場所が指定される。ファイル鍵生成部７０１において、入力された鍵パスワードと格納場所情報とから、ファイル鍵が生成され、ファイル暗号部１０４においてファイルが暗号化される。

【００４９】次に認証情報作成部１０５においては、入力された鍵パスワードの認証情報（例えばハッシュ値等）が作成され、暗号ファイルのヘッダ部に添付される。暗号処理部１１００では、格納場所指定部７００で指定された暗号ファイルの格納場所情報が、所定の暗号鍵で暗号化され、暗号ファイル１０７のヘッダに添付される。

【００５０】次に復号処理について述べる。鍵パスワード入力部２００において、例えばメモリカードにより鍵パスワードが入力される。入力された鍵パスワードは、認証部６００において、暗号ファイル１０７のヘッダに添付された鍵パスワード認証情報１０８と比較される。認証が正しく行われた場合、認証部６００からは鍵パスワードが出力され、認証に失敗すれば、認証に失敗した旨の情報が出力される。復号処理部１２００では、暗号ファイル１０７のヘッダ部に格納された格納場所情報１１０１が、所定の暗号鍵を用いて復号処理される。ファイル鍵生成部では、認証部６００での認証結果に基づき、認証が正しく行われた場合のみファイル鍵が生成され、ファイルの復号処理が行われる。

【００５１】実施の形態３では、暗号ファイルヘッダに格納場所の認証情報のみを格納することとしたが、本実施の形態では暗号ファイルヘッダに、格納場所情報を暗号化して格納した。これにより、暗号ファイルをフロッピー（登録商標）ディスク等の記憶媒体を経由して他のマシンへ移動した場合でも、ファイルの復号が可能である。

【００５２】（実施の形態５）図１３は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図１と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図１３において、１３００は装置のシリアル番号を抽出するシリアル番号抽出部、１３０１は鍵パスワードとシリアル番号とからファイル鍵を生成するファイル鍵生成部、１３０２は前記シリアル番号の認証情報を作成する認証情報作成部、１３０３は、シリアル番号の認証情報である。

【００５３】図１４は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図１２と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図１４において、１４００は装置のシリアル番号を抽出するシリアル番号抽出部、１４０１は抽出されたシリアル番号の認証を行う認証部、１４０２はファイル鍵を生成するファイル鍵生成部である。

【００５４】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【００５５】まず暗号処理について述べる。シリアル番号抽出部１３００では、ファイル暗号復号装置に付されているシリアル番号が抽出される。ファイル鍵生成部１３０１では、鍵パスワード入力部１００から入力された鍵パスワードと、シリアル番号抽出部１３００で抽出されたシリアル番号とに基づきファイル鍵が生成される。ファイル鍵の生成は、例えば図９において「格納場所情報」の代わりに「シリアル番号」を用いることで説明できる。あるいはシリアル番号の長さをn文字に固定しておくことで、図１５に示すように、鍵生成の流れを簡素化することもできる。ファイル鍵生成部１３０１において生成された鍵により、ファイルが暗号化される。認証情報作成部１０５では鍵パスワードの認証情報が作成され、認証情報作成部１３０２ではシリアル番号の認証情報が作成されて暗号ファイル１０７のヘッダに添付される。

【００５６】次に復号処理について述べる。シリアル番号抽出部１４００において、ファイル暗号復号装置のシリアル番号が抽出される。このシリアル番号は、認証部１４０１において、シリアル番号認証情報１３０３と照合される。認証に成功した場合、ファイル鍵生成部１４０２に対してシリアル番号が出力され、鍵パスワードとシリアル番号とに基づきファイル鍵が生成され、ファイルの復号が行われる。認証に失敗した場合は認証に失敗した旨の情報が出力され、ファイル鍵は生成されず、ファイルも復号されない。

【００５７】実施の形態３において、認証に失敗した場合に復号不能とすれば、例えば他のディレクトリへ暗号ファイルをコピーすれば、復号不能となるので、ファイルコピーに対するセキュリティレベルを向上できるというメリットが生じた。本実施の形態では、装置のシリアル番号を判別するので、例えばフロッピーディスク等の可搬媒体や、ネットワーク経由で他のマシンへファイル

THIS PAGE BLANK (USPTO)

としたが、鍵番号を暗号化して暗号ファイルのヘッダに添付することもできる。この場合の暗号および復号処理を図２０および図２１に示す。図２０において、図１６と同じ符号のものは同じ機能を有する。図２０において、２０００は暗号処理部、２００１は鍵番号情報である。暗号処理部２０００では、鍵番号入力部１６０１から入力された鍵番号を所定の鍵で暗号化する。暗号化された鍵番号は、鍵番号情報２００１として暗号ファイルのヘッダに添付される。

【００６９】次に復号時の処理について説明する。図２１において、２１００は復号処理部である。復号処理部２１００では、暗号ファイルに添付された鍵番号情報２００１を所定の鍵で復号化し、鍵番号が取り出される。

【００７０】このように、鍵番号が暗号ファイルのヘッダに添付されるので、鍵番号を入力することなく、復号ができる。

【００７１】（実施の形態７）図２２は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図１６と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図２２において、２２００は暗号ファイルの格納場所を指定する格納場所指定部、２２０１は格納場所の認証情報を作成する認証情報作成部、２２０２は格納場所の認証情報である。

【００７２】図２３は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図１６および図１７と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図２３において、２３００は暗号ファイルの格納場所を抽出する格納場所抽出部である。

【００７３】まず暗号処理について説明する。格納場所指定部２２００では、暗号ファイルを格納する場所の指定をユーザが行う。認証情報作成部２２０１で、格納場所の認証情報が作成され、格納場所認証情報２２０２として暗号ファイルのヘッダに添付される。

【００７４】次に復号処理について説明する。格納場所抽出部２３００において、暗号ファイルが格納されている場所の情報が抽出される。認証部１７００で暗号ファイルに添付された格納場所認証情報と比較され、一致した場合はファイル復号処理が行われ、一致しない場合はファイルの復号処理は行われない。

【００７５】このように構成することで、暗号ファイルのファイルコピーに対するセキュリティレベルを向上することができる。

【００７６】なお、上記説明では、格納場所の認証情報のみを暗号ファイルのヘッダに添付するとしたが、格納場所を所定の鍵で暗号化した情報をヘッダに添付してもよい。この場合を図２４および図２５を用いて説明する。図２４は暗号処理を示しており、図２２と同じ符号のものは同じ機能を有する。図２４において２４００は格納場所指定部の暗号処理を行う暗号処理部、２４０１

は暗号化された格納場所情報である。

【００７７】図２５は復号処理を示しており、図２３および図２４と同じ符号のものは同じ機能を有する。図２５において、２５００は格納場所情報２４０１を所定の鍵で復号する復号処理部である。

【００７８】このように構成することで、鍵番号の入力の手間がかからず、暗号および復号処理を行うことができる。

【００７９】また、実施の形態５で述べたように、装置のシリアル番号を暗号ファイルに添付してもよい。この様子を図２６および図２７を用いて説明する。

【００８０】図２６は暗号処理を示しており、図１６と同じ符号のものは同じ機能を有する。図２６において、２６００はシリアル番号抽出部、２６０１は認証情報作成部、２６０２はシリアル番号の認証情報である。

【００８１】図２７は復号処理を示しており、図１７および図２６と同じ符号のものは同じ機能を有する。図２７において、２７００はシリアル番号抽出部、２７０１はシリアル番号の認証を行う認証部である。

【００８２】シリアル番号抽出部２６００において、装置のシリアル番号が抽出される。認証情報作成部２６０１にてシリアル番号の認証情報が作成されて暗号ファイル１６０８のヘッダ部に添付される。復号時には、シリアル番号抽出部２７００で装置のシリアル番号が抽出され、認証部２７０１でファイルヘッダに添付されたシリアル番号認証情報２６０２と比較される。比較の結果一致すれば復号が行われ、一致しなければ復号は行われない。これにより、暗号時と異なる装置で復号することを防ぐことができる。

【００８３】

【発明の効果】以上のように、請求項１および２記載の発明によると、通常の暗号復号処理時はメモリカードなどの記録媒体に格納された暗号鍵が用いられるが、暗号鍵が鍵パスワードから生成されているので、メモリカード紛失などの緊急時でも、鍵パスワードの入力により復号を行うことができる。

【００８４】また請求項８および９記載の発明によると、ユーザ管理ファイルにより暗号鍵が管理されているので、通常にパソコンにログインする感覚でファイルの暗号復号処理を行うことができる。

【００８５】また請求項１４記載の発明によれば、メモリカード上に鍵パスワードを格納することにより、キーボード等から鍵パスワードを入力する手間を省くことができる。復号時にメモリカードを紛失した場合には、キーボード等から鍵パスワードを入力することでファイルの復号を行うことができる。また、この場合、メモリカードによるファイル復号を禁止することにより、紛失したメモリカードの悪用を防止することができる。

【００８６】また請求項１５記載の発明によれば、ファイルの使用目的に応じて鍵番号を設定できるので、複数

のファイルの管理が容易になる。

【００８７】また請求項１６記載の発明によれば、鍵パスワードから生成された暗号鍵に対して、同一の変換処理を繰り返して鍵を生成するので、簡単な処理で複数の暗号鍵を生成することができる。

【００８８】また請求項１７記載の発明によれば、鍵生成情報が、暗号ファイルの格納場所情報として与えられるので、鍵番号を覚えておく必要が無く、ファイルの格納場所と関連付けて鍵番号を管理できる。また他のディレクトリへ暗号ファイルをコピーした際に、復号を禁止できるので、ファイルのコピーに対するセキュリティレベルを向上することができる。

【００８９】また請求項２１記載の発明によれば、鍵生成情報が、装置のシリアル番号として与えられるので、フロッピーディスクやネットワーク経由で他の装置へファイルがコピーされた場合に復号を禁止することができる。

【００９０】また請求項２４記載の発明によれば、マスタユーザの暗号鍵に基づき一般ユーザの暗号鍵が生成されるので、一般ユーザが鍵パスワードを忘却した場合でも、マスタユーザが暗号鍵を生成することができる。またユーザ管理ファイルが何らかの要因で破損した場合でも、マスタユーザの鍵パスワードから一般ユーザの暗号鍵を生成することができる。

【図面の簡単な説明】

【図１】実施の形態１におけるファイル暗号処理のブロック図

【図２】実施の形態１におけるファイル復号処理のブロック図

【図３】鍵番号の説明図

【図４】鍵番号に基づく鍵生成のフロー図

【図５】実施の形態２におけるファイル暗号処理のブロック図

【図６】実施の形態２におけるファイル復号処理のブロック図

【図７】実施の形態３におけるファイル暗号処理のブロック図

【図８】実施の形態３におけるファイル復号処理のブロック図

【図９】格納場所情報に基づく鍵生成のフロー図

【図１０】格納場所情報の説明図

【図１１】実施の形態４におけるファイル暗号処理のブロック図

【図１２】実施の形態４におけるファイル復号処理のブロック図

【図１３】実施の形態５におけるファイル暗号処理のブロック図

【図１４】実施の形態５におけるファイル復号処理のブロック図

【図１５】シリアル番号に基づく鍵生成のフロー図

【図１６】実施の形態６におけるファイル暗号処理のブロック図

【図１７】実施の形態６におけるファイル復号処理のブロック図

【図１８】ユーザ管理ファイルの一例の説明図

【図１９】ユーザ管理ファイルの他の例の説明図

【図２０】実施の形態７における鍵番号に基づくファイル暗号処理のブロック図

【図２１】実施の形態７における鍵番号に基づくファイル復号処理のブロック図

【図２２】実施の形態７におけるファイル暗号処理のブロック図

【図２３】実施の形態７におけるファイル復号処理のブロック図

【図２４】実施の形態７における格納場所に基づくファイル暗号処理のブロック図

【図２５】実施の形態７における格納場所に基づくファイル復号処理のブロック図

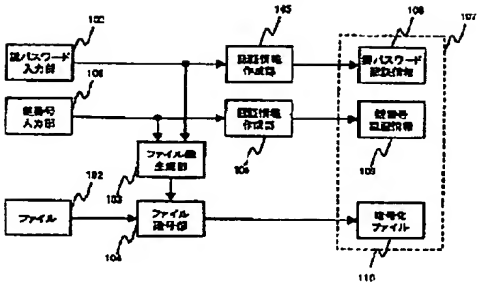
【図２６】実施の形態７におけるシリアル番号に基づくファイル暗号処理のブロック図

【図２７】実施の形態７におけるシリアル番号に基づくファイル復号処理のブロック図

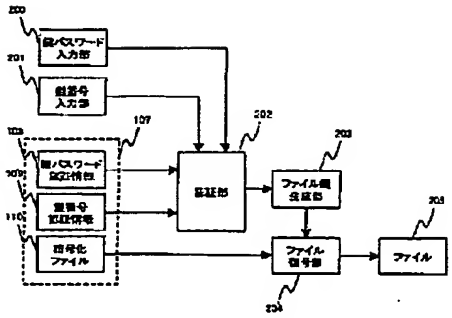
【符号の説明】

１００　鍵パスワード入力部
１０１　鍵番号入力部
１０２　ファイル
１０３　ファイル鍵生成部
１０４　ファイル暗号部
１０５　認証情報作成部
１０６　認証情報作成部
１０７　暗号ファイル
１０８　鍵パスワード認証情報
１０９　鍵番号認証情報
１１０　暗号化ファイル

【図１】



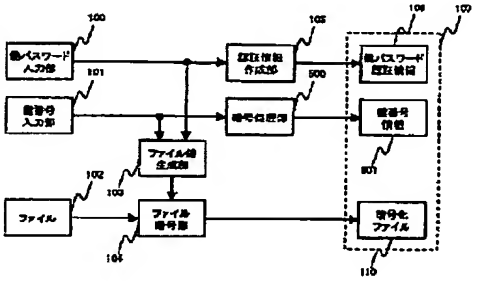
【図２】



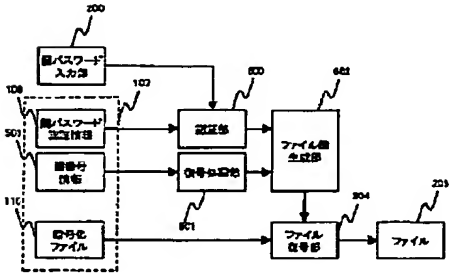
【図３】

個パスワード	A	B	----------	X
目的	会社用	個人用	----------	友人用
暗号鍵 1	自分のみ	自分のみ	----------	自分のみ
暗号鍵 2	プロジェクト用	全員用	----------	ごく親しい友人用
⋮	⋮	⋮	----------	⋮
暗号鍵 N	重要事項用	全員用	----------	友人一般用

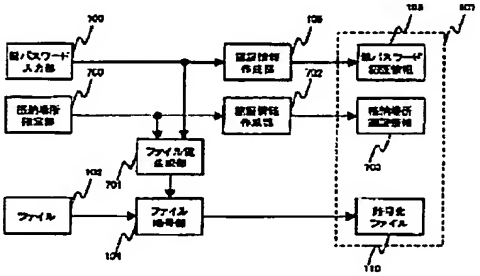
【図５】



【図６】



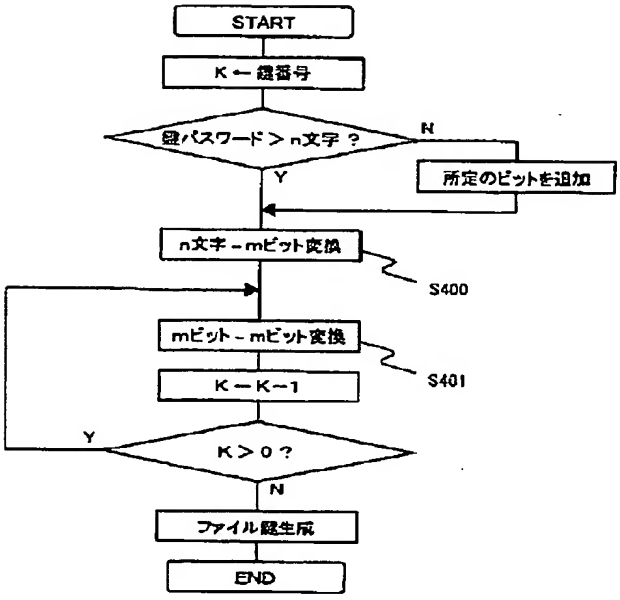
【図７】



【図１８】

ユーザ名	パスワード認証情報	個パスワード
ユーザA	H(PA)	K(A)
ユーザB	H(PB)	K(B)
⋮	⋮	⋮
ユーザN	H(PN)	K(N)

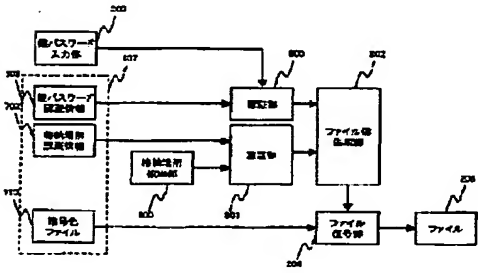
【図4】



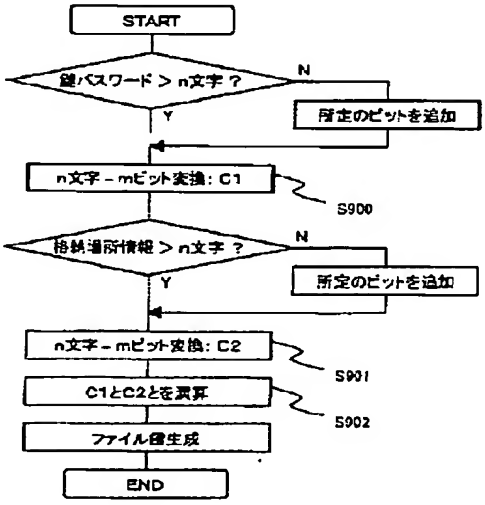
【図19】

スーパユーザ	H(P(S))	K(S)
ユーザA	H(P(A))	F(K(S), A)
ユーザB	H(P(B))	F(K(S), B)
⋮	⋮	⋮
ユーザN	H(P(N))	F(K(S), N)

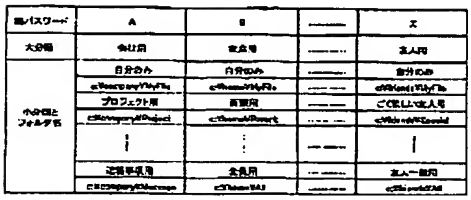
【図8】



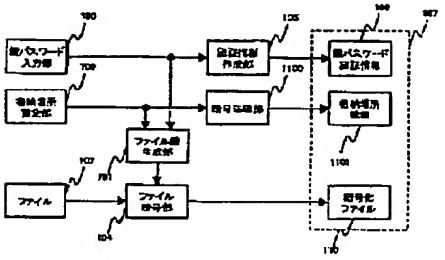
【図9】



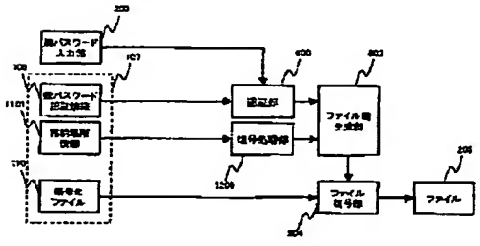
【図１０】



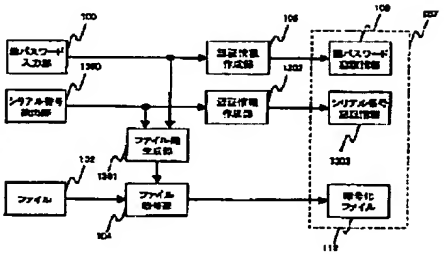
【図１１】



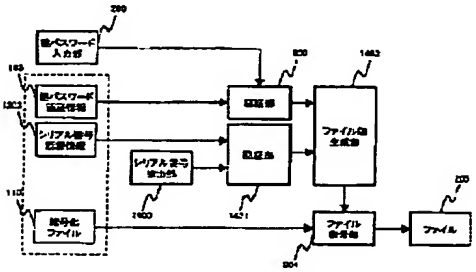
【図１２】



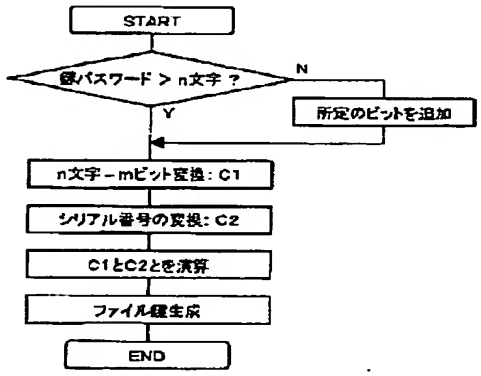
【図１３】



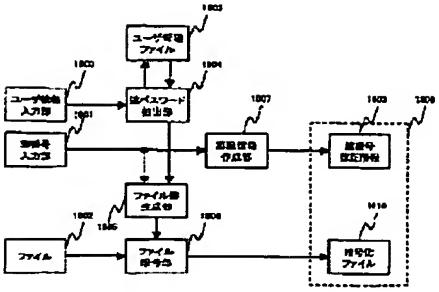
【図１４】



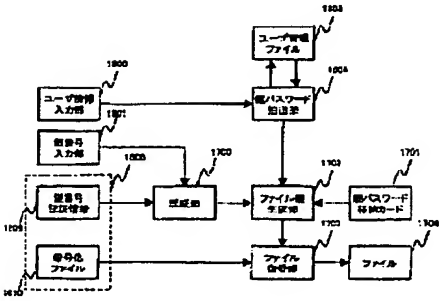
【図１５】



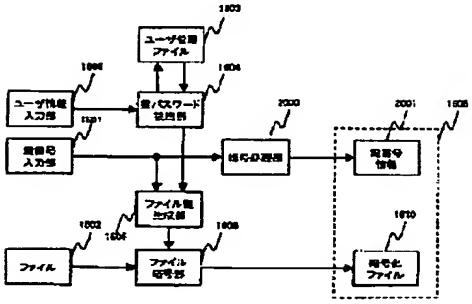
【図１６】



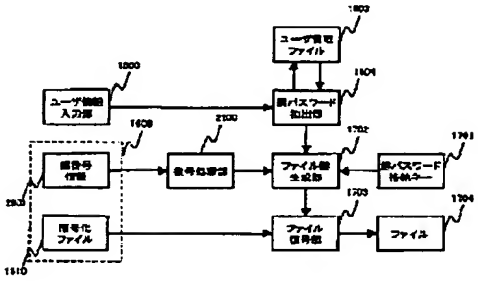
【図１７】



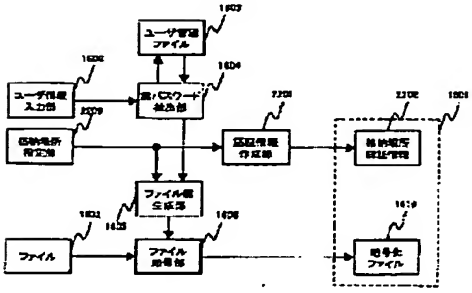
【図２０】



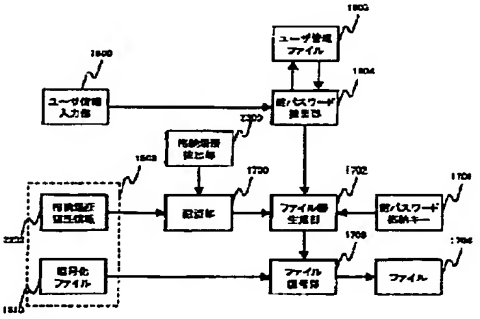
【図２１】



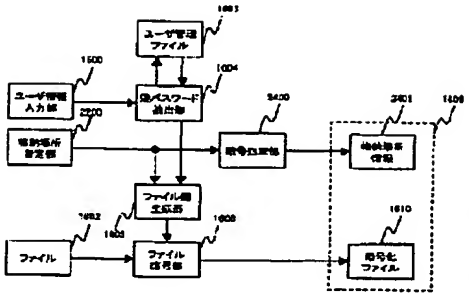
【図２２】



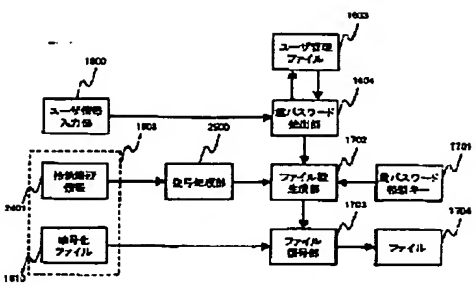
【図２３】



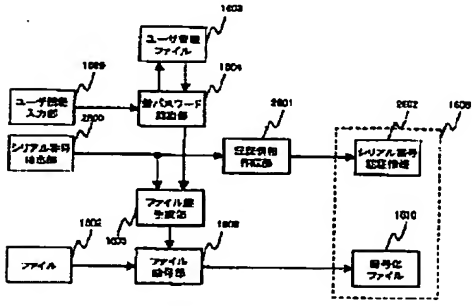
【図２４】



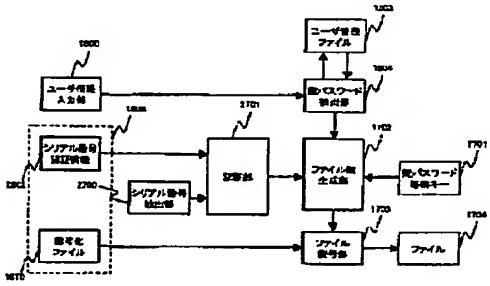
【図２５】



【図２６】



【図２７】



フロントページの続き

(51) Int. Cl.⁷	識別記号	FI	テーマコード（参考）
G09C 1/00	630	H04L 9/00	601Z

(72) 発明者 江村 里志
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72) 発明者 日高 紀幸
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72) 発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器産業株式会社内

Fターム（参考） 5B017 AA03 BA05 BA07 CA16
5B082 EA12 GA02 GA11
5J104 AA01 AA07 AA16 EA04 EA06
EA11 EA26 KA01 NA01 NA05
NA35 NA38 PA14